AIMMS ISO 27001:2022 - Statement of Applicability Version 2.0 Date 05-09-2023



Procession contents		Date 05-09-2023				Allvillaio
A			Control	Applicable?	Reason for inclusion / exclusion	Implemented?
Manual Processor Security Se			approved by management, published, communicated to and acknowledged by	Yes	Best Practices / Company Requirements	Yes
Assemblement of the company of the c		Information security roles and	intervals and if significant changes occur.			
Management furnishment of the control of the contro		responsibilities	according to the organization needs.			Yes
publishment directation of the prostocotion of an information of the prostocotion of the prostocotio	A.5.3	Segregation of duties		Yes	Best Practices / Company Requirements	Yes
Procedure of the content of the co	A.5.4	Management responsibilities		Yes	Best Practices / Company Requirements	Yes
Security of children with project interesting the project of the special production and professional security from the control of the special production and professional security from the control of the special production and professional production and p	A.5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes	Best Practices / Company Requirements	Yes
Section Section Process Control or projection Section	A.5.6	Contact with special interest groups		Yes	Best Practices / Company Requirements	Yes
As assistated work of entiremon and other assistant diseases.  As the developed and intermitation and control of the assistant diseases.  As the developed and intermitation and control of the assistant diseases.  As the developed and intermitation and control of the assistant diseases.  As the developed and supposed and the recreased particles as appropriate will climate all predictions and control of the assistant diseases.  As the developed and supposed and the recreased particles as appropriate will climate all predictions and control of the assistant diseases.  As the developed and control of the assistant dis	A.5.7	Threat intelligence		Yes	Risk analysis	Yes
Assessment states to that be developed and materiance. The process of the process	A.5.8			Yes	Best Practices / Company Requirements	Yes
Substitute seasons and accordance assets that has believable, documented and implemented.  A.5.11 Record of seasons approaches a season and accordance assets that has believable and accordance assets that has believable and appropriate and return and the approaches and accordance assets that has believable and approaches and accordance assets that has believable and approaches and accordance assets that has believable and approaches and accordance assets that has been accor	A.5.9			Yes	Best Practices / Company Requirements	Yes
Act   Act   Confliction of information   Configuration   Con	A.5.10			Yes	Best Practices / Company Requirements	Yes
As 25 Classification of information manufactor washing consolination security reviews of the opportunities to accordance from the information security reviews of the company from the committed in the committed	A.5.11	Return of assets	organization's assets in their possession upon change or termination of their	Yes	Best Practices / Company Requirements	Yes
A.5.12 Access curiors  A.5.24 Access curiors  A.5.25 Access curiors  A.5.26 Access curiors  A.5.27 Access curiors  A.5.28 Access curiors  A.5.29 Access curiors  A.5.29 Access curiors  A.5.20 Access curiors  A.5.20 Access curiors  A.5.21 Access curiors  A.5.22 Access curiors  A.5.23 Access curiors  A.5.24 Access curiors  A.5.25 Access curiors  A.5.26 Access curiors  A.5.27 Access curiors  A.5.27 Access curiors  A.5.28 Access regines  A.5.29 Access regines  A.5.20 Access regines  A.5.21 Access regines  A.5.22 Access regines  A.5.22 Access regines  A.5.23 Access regines  A.5.24 Access regines  A.5.25 Access regines  A.5.26 Access regines  A.5.27 Access regines  A.5.27 Access regines  A.5.28 Access regines  A.5.29 Access regines  A.5.20 Access regines  Access regines  A.5.20 Access regines  Access regines  A.5.20 Access regines  Access regines access regines  Access regines  Access regines  Access regines access regines  Access regines access regines  Access regines access regines  Access regines access regines  Access regines access regines  Access regines access regines  Access regines access regines  Access regines access regines  Access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access regines access	A.5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant	Yes	Best Practices / Company Requirements	Yes
A.5.12 Information transfer rules, procedures, or agreements shall be in place for all types of transfer fedilises with the organization and effective members of the place for all types of transfer fedilises with the organization and effective members.  A.5.13 Access control  A.5.16 Identify missagement  The full fill register of the place o	A.5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed	Yes	Best Practices / Company Requirements	Yes
Section   Sect						
A.5.15 Access control  A.5.26 Secretary for a special process and a set established and implemented band on hous meas and process. Access registres and proc	A.5.14	Information transfer	organization and other parties.	Yes	Best Practices / Company Requirements	Yes
A.5.12 Authentication information by a management process, including advising personned in appropriate by a management process, including advising personned in appropriate by a management process, including advising personned in appropriate by a management process, including advising personned in appropriate by a management process, including advising personned in appropriate by a management process, including advising personned in appropriate provisioned, advisional process and advisional process control to processes or appetition processes for appetition processes for appetitions, use, management and exist from cloud services supply and communication security includent managements  A.5.2.2 Information security for use of cloud services be established in appetition processes for appetitions, use, management and exist from cloud services supply and appetition processes for appetitions, use, management and exist from cloud services supply appetition processes for appetitions, use, management and exist from cloud services supply appetition security inclined in appetition processes for appetitions, use, management and exist from cloud services and services supply appetition processes for appetitions, use, management and exist from cloud services and services a			assets shall be established and implemented based on busi ness and information security requirements.			Yes
A.5.18 Acces rights		·	Allocation and management of authentication information shall be controlled			Yes
specific policy on and rules for access control.  A 5.19 Information security in supplier relationships of the security in supplier specifies and procedures shall be defined and implemented to manage the information security within supplier specifies and procedures shall be established and agreed with each supplier specifies on the type of supplier relationship.  A 5.20 Montaining information security within and communication technology (ICT) supply shall referred to manage the information of security in the season of the type of supplier relationship.  A 5.21 Information security in the information of security in the season of the type of supplier relationship.  A 5.22 Information security in the information in security in security in the season of security for use of cloud services and procedures shall be defined and implemented to manage the process and procedures shall be defined and implemented to manage the information security incidents and the season of security indicates the security ind	A.5.17	Authentication information	handling of authentication information.	Yes	Best Practices / Company Requirements	Yes
services.  A 5.20 Addressing information security within experiments shall be established and agreed with each supplier pased on the type of supplier relationship.  A managing information security in the information information security in the information and information security in the information information security in the information security risks associated with the ICT products and services supply and communication technology (ICT) supply claim.  A 5.20 Montal of the information security in the information security risks associated with the ICT products and services supply and supplier information security practices and services supplier information security practices and services delivers.  A 5.21 Information security incident management in production of security incidents or product in the information security incident with the information security incident with the information security incidents or information security incidents.  A 5.20 Information security incidents or information security incidents.  A 5.21 Response to information security incidents.  A 5.22 Information security incidents.  A 5.23 Collection of evidence information security incidents.  A 5.24 Information security incidents.  A 5.25 Information security incidents.  A 5.26 Information security incidents.  A 5.27 Information security incidents.  A 5.28 Information security incidents.  A 5.29 Information security incidents.  A 5.20 Information security incidents.  A 5.21 Information security incidents.  A 5.22 Information information information information i	A.5.18	Access rights	specific policy on and rules for access control.	Yes	Best Practices / Company Requirements	Yes
with each supplier based on the type of supplier relationships.  As 22 Montoring, review and change management information accurity in the organization shall regularly monitor, review, evaluate and manage change of supplier services.  As 23 Information security incident management of supplier services and precent eleviery.  As 24 Montoring, review and change management of supplier services and precent eleviery.  As 25 Information security incident management of supplier services and service security practices and service delivery.  As 26 Response to information security incident management processes, roles and responsibilities.  As 27 Information security incident management processes information security incident shall plan and prepara for managing information security would be calculated in accordance with the organization shall plan and prepara for managing information security would be calculated in accordance with the organization shall security events and security events and security incidents with the organization shall security events and security incidents and preparation security incidents.  As 28 Response to information security incidents.  As 29 Information security incidents information security incidents.  As 20 Information security incidents.  As 20 Information security incidents.  As 20 Information security incidents.  As 21 Information security incidents.  As 22 Information security incidents.  As 23 Information security incidents.  As 24 Information security incidents.  As 25 Information security incidents.  As 26 Information security incidents shall be responsibilities.  As 27 Information security incidents shall be responsibilities.  As 28 Information security incidents shall be responsibilities.  As 29 Information security incidents shall be responsibilities.  As 29 Information security during disruption information security incidents shall be responsibilities.  As 29 Information security during disruption information security incidents shall be responsibilities.  As 20 Information security	A.5.19	Information security in supplier relationships	information security risks associated with the use of supplier's products or	Yes	Best Practices / Company Requirements	Yes
A 5.22 Information information  A 5.23 Information information  A 5.24 Information security rinds associated with the Cirproducts and service supply chain.  A 5.25 Information security rinds associated with the Cirproducts and service supply chain.  A 5.26 Information security for use of cloud services from supplier services.  A 5.27 Information security for use of cloud services from supplier services from supplier services.  A 5.28 Information security incident management planning and preparation.  A 5.29 Information security incident management planning and preparation.  A 5.20 Seasoner and decision on information.  A 5.21 Seasoner information security incident.  A 5.22 Learning from Information security incidents.  A 5.23 Learning from Information security incidents.  A 5.24 Learning from Information security incidents.  A 5.25 Learning from Information security incidents.  A 5.26 Response to Information security incidents.  A 5.27 Learning from Information security incidents.  A 5.28 Collection of evidence  The organization shall be responsed to in accordance with the companization shall be responsed to in accordance with the companization shall be responsed to in accordance with the companization shall be responsed to in accordance with the companization shall be responsed to in accordance with the companization shall plan the responsed to in accordance with the companization shall plan the responsed to in accordance with the companization shall plan the responsed to in accordance with the companization shall plan the responsed to in accordance with the companization shall plan the responsed to in accordance with the companization shall plan the vice of the information security incidents.  A 5.28 Collection of evidence  The organization shall plan how to maintain information security at an approach to information security and the organization shall plan how to maintain information security at an approach to maintain information security and the organization shall plan how to maintain information and teste	A.5.20	supplier agreements	, ,	Yes	Best Practices / Company Requirements	Yes
A 5.22 of Supplier services and change management in processes for acquisition, sue, management and eart from cloud services shall be processed for acquisition, use, management and eart from cloud services shall be seablished in accordance with the organization shall plan and preparation from the organization shall plan and preparation security incident management processes, and the organization shall plan and preparation security incident management processes, roles and responsibilities.  A 5.26 Response to information security incident management processes, roles and responsibilities.  A 5.27 Learning from information security incident management processes, roles and responsibilities.  A 5.28 Assessment and decision on information information security incident management processes, roles and responsibilities.  A 5.29 Learning from information security incidents shall be septoned to in accordance with the documented procedures.  A 5.20 Learning from information security incidents shall be septoned to in accordance with the documented procedures.  A 5.20 Lollection of evidence  A 5.21 Learning from information security incidents shall be septoned to in accordance with the documented procedures.  A 5.22 Learning from information security incidents shall be septoned to in accordance with the documented procedures.  A 5.23 Learning from information security incidents shall be septoned to in accordance with the documented procedures.  A 5.24 Learning from information security incidents shall be septoned to in accordance with the documented procedures.  A 5.25 Learning from information security incidents shall be information security controls.  A 5.26 Learning from information security incidents shall be information security at an administration shall plan how to maintain information security at an administration shall plan how to maintain information security at an administration shall plan how to maintain information security at an administration shall plan how to maintain information security at an administration	A.5.21	information and communication technology (ICT) supply-	information security risks associated with the ICT products and services supply	Yes	Best Practices / Company Requirements	Yes
A.5.24 Information security for use of cloud services be established in accordance with the organization's information security requirements.  A.5.24 Information security incident management planning and preparation Janning and preparation Jannin	A.5.22	Monitoring, review and change management		Yes	Best Practices / Company Requirements	Yes
h.5.25 planning and preparation incident management processes, roles and responsibilities.  A5.26 planning and preparation incident management processes, roles and responsibilities.  A5.27 planning and preparation security incidents and because the object and procedures in formation security events and decide if they are to be categorized as information security events and decide if they are to be categorized as information security incidents.  A5.27 planning from information security incidents shall be responsed to in accordance with the documented procedures.  A5.28 planning from information security incidents shall be used to strengthen and improve the information security incidents shall be used to strengthen and improve the information security controls.  A5.29 planning from information security during disruption information security events.  A5.20 planning from information security during disruption information security events.  A5.21 planning from information security during disruption information security events.  A5.22 planning from information security during disruption information security events.  A5.23 planning from information security during disruption information security events.  A5.24 planning from information security during disruption information security events.  A5.25 planning from information security during disruption information security at an appropriate level during disruption information security at a security at a security and	A.5.23	Information security for use of cloud services	be established in accordance with the organization's information security	Yes	Best Practices / Company Requirements	Yes
A.S.25 security events to be categorized as information security incidents. A.S.26 Response to information security incidents of information security incidents shall be responded to in accordance with the documented procedures. A.S.27 Learning from information security incidents shall be responded to in accordance with the documented procedures. A.S.28 Collection of evidence  A.S.28 Collection of evidence  A.S.29 Information security during disruption  A.S.20 Information security during disruption  A.S.20 Information security during disruption  A.S.20 Information security during disruption  A.S.21 Legal, statutory, regulatory and contractual regular membras shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.  A.S.21 Intellectual property rights  A.S.22 Intellectual property rights  A.S.23 Protection of records  A.S.24 Privacy and protection of personal identified information security and the organization shall implement appropriate procedures to protect intellectual property rights.  A.S.23 Independent review of information security incidents shall be identified, documented and kept up to date.  The organization shall implement appropriate procedures to protect organization shall ineplement appropriate procedures to protect intellectual property rights.  A.S.23 Independent review of information security and the organization shall ineplement appropriate procedures to protect organization shall ineplement appropriate procedures for Placco	A.5.24		incidents by defining, establishing and communicating information security	Yes	Risk analysis	Yes
A.5.26 Learning from information security incidents A.5.27 Learning from information security incidents A.5.28 Collection of evidence  Collection of evidence  Collection of evidence  Information security events.  A.5.29 Information security during disruption  A.5.20 Information security during disruption  A.5.20 Information security during disruption  A.5.30 ICT readiness for business continuity  ICT readiness for business continuity  ICT readiness for business continuity  Legal, statutory, regulatory and contractual requirements  A.5.31 Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall implement appropriate procedures to protect  Intellectual property rights  The organization shall be protected from loss, destruction, falsification, unauthorized access and unauthorized releases.  The organization shall dentify and meet the requirements regarding the preservation of privacy and protection of Pla according to applicable laws and regulations and contractual requirements.  The organization shall including people, processes and technologies shall be reviewed independently at planned intervols, or when significant changes occur.  The organization shall be regularly reviewed.  A.5.36 Compliance with policies, rules and compliance with the organization is informati	A.5.25			Yes	Risk analysis	Yes
A.5.27 Learning from information security incidents strengthen and improve the information security controls.  A.5.28 Collection of evidence Information security events.  A.5.29 Information security during disruption The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security during disruption.  A.5.30 ICT readiness for business continuity CICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.  A.5.31 Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.  A.5.32 Intellectual property rights The organization shall implement appropriate procedures to protect intellectual property rights.  A.5.33 Protection of records Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.  A.5.34 Privacy and protection of personal destination of the preservation of privacy and protection of personal regulations and contractual requirements.  A.5.35 Independent review of information security  A.5.36 Compliance with policies, rules and compliance with the organization's information security policies, rules and and made available to personnel who need them.  A.5.36 Compliance with policies, rules and Compliance with the organization's information processing facilities shall be documented  A.5.37 Documented operating procedures  A.5.38 Documented operating procedures  A.5.39 Documented operating procedures  A.5.30 Compliance with policies, rules and and made available to personnel who need them.	A.5.26	Response to information security incidents	documented procedures.	Yes	Risk analysis	Yes
A.5.28 Collection of evidence ident tification, collection, acquisition and preservation of evidence related to information security events.  A.5.29 Information security during disruption  The organization shall plan how to maintain information security at an appropriate level during disruption.  A.5.30 ICT readiness for business continuity  Legal, statutory, regulatory and contractual requirements.  Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.  A.5.31 Intellectual property rights  A.5.32 Intellectual property rights  The organization shall implement appropriate procedures to protect intellectual property rights.  A.5.33 Protection of records  Risk analysis  The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PIP acquirements.  The organization shall identify and meet the requirements regarding the preservation of PIP according to applicable laws and regulations and contractual requirements.  The organization shall identify and meet the requirements recording to applicable laws and regulations and contractual requirements.  The organization shall identify and meet the requirements recording to applicable laws and regulations and contractual requirements.  The organization shall identify and meet the requirements recording to applicable laws and regulations and contractual requirements.  The organization shall identify and meet the requirements recording to applicable laws and regulations and contractual requirements.  The organization shall identify and meet the requirements regarding the previewed independently at planned intervals, or when significant changes occur.  A.5.36 Compliance with policies, rules and standards for information security policy, topic-specific policies, rules and standards shall be regularly reviewed.  A.5.37 Documented operating procedures  Documented operating procedur	A.5.27	Learning from information security incidents	strengthen and improve the information security controls.	Yes	Risk analysis	Yes
A.5.29 Information security during disruption  The organization shall plan how to maintain information security at an appropriate level during disruption.  A.5.30 ICT readiness for business continuity  Legal, statutory, regulatory and contractual business continuity objectives and ICT continuity requirements.  Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements frequirements all be identified, documented and kept up to date.  A.5.32 Intellectual property rights  The organization shall implement appropriate procedures to protect intellectual property rights.  A.5.33 Protection of records  Privacy and protection of personal identifiable information (PII)  The organization shall identify and meet the requirements regarding the preservation of privacy and protection of personal identifiable information (PII)  The organization shall identify and meet the requirements regarding the preservation of privacy and protection of personal identifiable information (PII)  The organization shall identify and meet the requirements regarding the preservation of privacy and protection of priv	A.5.28	Collection of evidence	iden tification, collection, acquisition and preservation of evidence related to	Yes	Risk analysis	Yes
A.5.30 Ict readiness for business continuity business continuity objectives and ICT continuity requirements.  A.5.31 Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements A.5.32 Intellectual property rights  A.5.33 Protection of records  A.5.34 Privacy and protection of personal identifiable information (PII)  A.5.35 Independent review of information security  A.5.36 Compliance with policies, rules and Standards for information security  A.5.36 Documented operating procedures  Description of public information security  Description of public information security  Description of privacy and protection of personal identifiable information security  Description of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements regarding the protection of PII according to applicable laws and regulations requirements regarding the	A.5.29	Information security during disruption	The organization shall plan how to maintain information security at an	Yes	Risk analysis	Yes
A.5.31 Legal, statutory, regulatory and tontractual requirements  A.5.32 Intellectual property rights  A.5.33 Intellectual property rights  A.5.34 Protection of records  A.5.35 Privacy and protection of personal identifiable information (PII)  A.5.35 Independent review of information security  A.5.36 Compliance with policies, rules and standards for information security  A.5.37 Documented operating procedures  Information security and the organization's approach to mean gling information security policies, rules and standards for information security  Operating procedures  Information security and the organization's approach to managing information security policies, rules and standards for information security  Operating procedures  A.5.37 Documented operating procedures  Information security and the organization's approach to managing information security policies, rules and standards for information security  Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	A.5.30	ICT readiness for business continuity		Yes	Risk analysis	Yes
A.5.32 Intellectual property rights  The organization shall implement appropriate procedures to protect intellectual property rights.  A.5.33 Protection of records  Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.  A.5.34 Privacy and protection of personal identifiable information (PII)  The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.  The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.  A.5.36 Compliance with policies, rules and Standards for information security policies, rules and standards for information security policies, rules and standards shall be regularly reviewed.  A.5.37 Documented operating procedures  The organization including people, processes and technologies shall be regularly reviewed.  Compliance with policies, rules and Standards shall be regularly reviewed.  Operating procedures for information processing facilities shall be documented and made available to personnel who need them.  Yes  Best Practices / Company Requirements  Prescription (PII)  Prescription (PII)  Prescription (PII)  Prescription (PII)  Prescription (PII)  Prescription (PII)  Prescription (PIII)  P	A.5.31		information security and the organization's approach to meet these	Yes	Laws & Regulations	Yes
A.5.33 Protection of records Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.  A.5.34 Privacy and protection of personal identifiable information (PII)  A.5.35 Independent review of information security  A.5.36 Compliance with policies, rules and standards for information security  A.5.37 Documented operating procedures  Risk analysis  Yes Risk analysis  Laws & Regulations  Yes Laws & Regulations  Yes Laws & Regulations  Laws & Regulations  Yes Practices / Company Requirements  Yes Best Practices / Company Requirements  Operating procedures or information security policy, topic-specific policies, rules and standards for information security  Operating procedures or information information and made available to personnel who need them.	A.5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect	Yes	Risk analysis	Yes
A.5.34 Privacy and protection of personal identifiable information (PII) preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.  A.5.35 Independent review of information security  Independent review of information security  A.5.36 Compliance with policies, rules and standards for information security policies, rules and standards for information security  A.5.37 Documented operating procedures  A.5.38 Documented operating procedures  A.5.39 Documented operating procedures  A.5.30 Documented oper	A.5.33	Protection of records	access and unauthorized release.	Yes	Risk analysis	Yes
A.5.35 Independent review of information security  A.5.36 Compliance with policies, rules and standards for information security  A.5.37 Documented operating procedures  The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.  Compliance with policies, rules and Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.  A.5.37 Documented operating procedures  Operating procedures for information processing facilities shall be documented and made available to personnel who need them.  The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed, accurately approach intervals, or when significant changes occur.  Yes  Best Practices / Company Requirements	A.5.34		preservation of privacy and protection of PII according to applicable laws and	Yes	Laws & Regulations	Yes
A.5.36 Compliance with policies, rules and standards for information security  A.5.37 Documented operating procedures  Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.  Operating procedures  Operat	A.5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes	Yes	Best Practices / Company Requirements	Yes
A.5.37 Documented operating procedures Operating procedures or information processing facilities shall be documented and made available to personnel who need them.  Operating procedures for information processing facilities shall be documented Yes Best Practices / Company Requirements	A.5.36		Compliance with the organization's information security policy, topic-specific	Yes	Best Practices / Company Requirements	Yes
	A.5.37		Operating procedures for information processing facilities shall be documented	Yes	Best Practices / Company Requirements	Yes
A6 People controls  Background verification checks on all candidates to become personnel shall be	A6	People controls	Background verification checks on all candidates to become personnel shall be			
A.6.1 Screening consideration applicable laws, regulations and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	A.6.1	Screening	carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed	Yes	Risk analysis	Yes

AIMMS ISO 27001:2022 - Statement of Applicability Version 2.0 Date 05-09-2023



	Date 05-09-2023			I	
Section	Торіс	Control	Applicable?	Reason for inclusion / exclusion	Implemented?
A.6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Yes	Best Practices / Company Requirements	Yes
A.6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Yes	Best Practices / Company Requirements	Yes
A.6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Yes	Best Practices / Company Requirements	Yes
A.6.5	Responsibilities after termination or change of employment	Information security poincy violation.  Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Yes	Risk analysis	Yes
A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organ ization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Yes	Risk analysis	Yes
A.6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Yes	Risk analysis	Yes
A.6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Yes	Risk analysis	Yes
A7	Physical controls				
A.7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Yes	Risk analysis	Yes
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Yes	Risk analysis	Yes
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and	Yes	Risk analysis	Yes
		implemented.			
A.7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.  Protection against physical and environmental threats, such as natural	Yes	Risk analysis	Yes
A.7.5	Protecting against physical and environmental threats	disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Yes	Risk analysis	Yes
A.7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	No	AIMMS staff do not work physically in datacenters. All actions are performed via remote access.	N/A
A.7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Yes	Risk analysis	Yes
A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes	Risk analysis	Yes
A.7.9 A.7.10	Security of assets off-premises Storage media	Off-site assets shall be protected.  Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Yes Yes	Risk analysis Risk analysis	Yes Yes
A.7.11	Supporting utilities	Information processing facilities shall be protected from power failures and	Yes	Risk analysis	Yes
A.7.12	Cabling security	other disruptions caused by failures in supporting utilities.  Cables carrying power, data or supporting information services shall be	Yes	Risk analysis	Yes
A.7.13	Equipment maintenance	protected from interception, interference or damage.  Equipment shall be maintained correctly to ensure availability, integrity and	Yes	Best Practices / Company Requirements	Yes
A.7.14	Secure disposal or re-use of equipment	confidentiality of information.  Items of equipment containing storage media shall be verified to en sure that any sensitive data and licensed software has been removed or securely	Yes	Risk analysis	Yes
		overwritten prior to disposal or re-use.			
A8	Technological controls	Information stored on, processed by or accessible via user end point devices		<b>.</b>	
A.8.1	User end point devices	shall be protected. The allocation and use of privileged access rights shall be restricted and	Yes	Risk analysis	Yes
A.8.2	Privileged access rights	managed.	Yes	Risk analysis	Yes
A.8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	Yes	Risk analysis	Yes
A.8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Yes	Risk analysis	Yes
A.8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes	Risk analysis	Yes
A.8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes	Risk analysis	Yes
A.8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes	Risk analysis	Yes
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	Yes	Best Practices / Company Requirements	Yes
A.8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	Yes	Best Practices / Company Requirements	Yes
A.8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	Yes	Risk analysis	Yes
A.8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Yes	Laws & Regulations	Yes
A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, net works and any other devices that process, store or transmit sensitive information.	Yes	Risk analysis	Yes
A.8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Yes	Risk analysis	Yes
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Risk analysis	Yes
A.8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	Yes	Risk analysis	Yes
A.8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential infor mation security incidents.	Yes	Risk analysis	Yes
A.8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes	Best Practices / Company Requirements	Yes
A.8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and	Yes	Risk analysis	Yes
A.8.19	Installation of software on operational	application controls shall be restricted and tightly controlled.  Procedures and measures shall be implemented to securely manage software	Yes	Risk analysis	Yes
	systems	installation on operational systems.  Networks and network devices shall be secured, managed and controlled to			
A.8.20	Networks security	protect information in systems and applications.	Yes	Risk analysis	Yes

AIMMS ISO 27001:2022 - Statement of Applicability Version 2.0 Date 05-09-2023



				I .	
Section	Торіс	Control	Applicable?	Reason for inclusion / exclusion	Implemented?
A.8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	Yes	Risk analysis	Yes
A.8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	Yes	Risk analysis	Yes
A.8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes	Risk analysis	Yes
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	Yes	Risk analysis	Yes
A.8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	Yes	Contractual Agreements	Yes
A.8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	Yes	Risk analysis	Yes
A.8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	Yes	Contractual Agreements	Yes
A.8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes	Contractual Agreements	Yes
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	Yes	Contractual Agreements	Yes
A.8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	Yes	Best Practices / Company Requirements	Yes
A.8.31	Separation of development, test and production environments	Development, testing and production environments shall be separated and secured.	Yes	Risk analysis	Yes
A.8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	Yes	Best Practices / Company Requirements	Yes
A.8.33	Test information	Test information shall be appropriately selected, protected and managed.	Yes	Laws & Regulations	Yes
A.8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of op erational systems shall be planned and agreed between the tester and appropriate management.	Yes	Risk analysis	Yes